Week Two

1 Proof Structures and Strategies

While we're not completely finished with the logic itself, we have covered enough to start looking at how it is applied in a mathematical setting. (The word "mathematical" should be taken in the broad sense, encompassing the mathematical sciences in general.) The formal process of constructing a truth table or a two-column deduction is left behind. Mathematical proofs are sketches, and are typically written in paragraph form. The nevertheless have their roots in the logic.

1.1 Inference

We need the notion of an *inference rule*. The best-known inference rule, which in the less-is-more tradition is really the only one we need, is Modus Ponens. Consider the following truth table:

P	Q	$(P$	$\wedge$	$(P$	$\Rightarrow$	$Q))$	$\Rightarrow$	Q
F	F	F	F	F	T	F	**T**	F
F	T	F	F	F	T	T	**T**	F
T	F	T	F	T	F	F	**T**	F
T	T	T	T	T	T	T	**T**	T

Based on the column of boldface T's, we can conclude that $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$ is true *regardless of the truth values of P and Q*. Such a proposition is called a *tautology*. Repackaged as an inference rule, this particular one is called Modus Ponens. Suppose, then, that we want to prove Q. If we happen to know that $P \Rightarrow Q$ is true, and if we know that P is true, then we're done: Q must be true. In this approach, either P or $P \Rightarrow Q$ might be a theorem that is at our disposal.

1.2 Direct Proof of an Implication

More often, we are faced with proving $P \Rightarrow Q$ on our own. Recalling the truth table for $P \Rightarrow Q$, we realize that it is pointless to consider the cases in which P is false, since the implication is always true in these cases. The only interesting cases are the two in which P is true, since then the truth of the implication depends upon the truth of Q. We must show that if P is true, then Q cannot be false. In a direct proof of $P \Rightarrow Q$, we begin by assuming that P is true. We then look for any available tools to assist us in proving that Q must follow.

For example, suppose we want to prove that if n is an even integer, then n^2 is also even. The direct approach would begin with the assumption that n is even. By definition, this means that $n = 2k$ for some integer k. Elementary algebra then gives us $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Since $2k^2$ is an integer, it follows that n^2 is even, and we're done.

When starting a direct proof, remember to assume the hypothesis. Then use definitions, theorems, and inference to blaze a trail to the conclusion. Once you arrive there, you're done.

1.3 Indirect Proof of an Implication

There are times when we assume the hypothesis of an implication and simply can't find a path to the conclusion. Sometimes we have better success using the contrapositive. For example, suppose that we want to prove the converse of the implication above, i.e., that if n^2 is even, so is n. We begin the direct attempt by assuming that n^2 is even. This means that $n^2 = 2k$ for some integer k. It then follows that $n = \sqrt{2k}$. What now? We have nothing to justify the claim that $\sqrt{2k}$ is even. So we abandon the direct approach. The contrapositive of our implication is that if n is odd, so is n^2. We assume that n is odd, which means that $n = 2k+1$ for some $n \in \mathbf{Z}$. It follows that $n^2 = (2k+1)^2 = 2(2k^2+2k)+1$, which is clearly odd. By contraposition, we have what we wanted: if n^2 is even, so is n. □

1.4 Proof By Contradiction

It is not the case that we prove only implications. Sometimes we must construct a proof for a claim that is difficult to cast as an implication in a useful way. The solution sometimes lies in what is called Proof by Contradiction. This method is rooted in another tautology:

P	$(\neg P$	$\Rightarrow$	$\mathbf{F})$	$\Rightarrow$	P
F	T	F	F	$\mathbf{T}$	F
T	F	T	F	$\mathbf{T}$	T

The strategy is to prove P by first assuming $\neg P$ and then deriving a contradiction. Recall that a contradiction is any proposition of the form $Q \wedge \neg Q$. For our example, we'll use a classic proof that $\sqrt{2}$ is irrational. Suppose, by way of contradiction, that $\sqrt{2}$ is rational. By definition of rational number, we have $\sqrt{2} = a/b$ for integers a and b ($b \neq 0$). Without loss of generality assume that a/b is in lowest terms (we could always add the step of putting a/b in lowest terms, but we know that it can be done so we might as well assume that it has *been* done.) Our assumption that $\sqrt{2} = a/b$ gives us $a^2 = 2b^2$, which implies that a^2 is even. By a preceding result, we know that a is even. Writing $a = 2j$, we now have $4j^2 = 2b^2$, but then $b^2 = 2j^2$ is even. Applying our prevous result once more, we have b even. But now both a and b are even, which contradicts the assumption that a/b is in lowest terms. What started all this trouble? Our assumption that $\sqrt{2}$ was rational. We abandon the assumption, concluding that $\sqrt{2}$ is irrational. □

2 Logical Equivalence

In the preceding section, we were introduced to the notion of tautology. This led to the inference rule known as Modus Ponens. There are other ways in which tautologies can be

useful. Consider the biconditional form, $P \Leftrightarrow Q$. A glance at the truth table for $P \Leftrightarrow Q$ show that is true only when P and Q have the same truth value. For primitive P and Q, this doesn't always happen. What about compound P and Q?

2.1 Tautology and Equivalence

For example, consider the biconditional form,

$$\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q).$$

If we construct the truth table for this biconditional, we find that it is a tautology. This establishes the *logical equivalence* of $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$. The author frequently uses a new logical operator to indicate this, replacing $\Leftrightarrow$ with $\equiv$. So we will henceforth write $P \equiv Q$ only when $P \Leftrightarrow Q$ is a tautology. The equivalence established above is one of a pair of *DeMorgan's Laws*. The other is formed by interchanging conjunction with disjunction, obtaining

$$\neg(P \vee Q) \equiv (\neg P \wedge \neg Q).$$

2.2 The Replacement Principle

How can we exploit logical equivalence? The answer is called the *Replacement Principle*, which is as follows: Suppose that S, S_1, and S_2 are propositions, and that $S_1 \equiv S_2$. If S' is obtained from S by replacing one or more occurences of S_1 with occurrences of S_2, then $S \equiv S'$.

For example, the first DeMorgan law discussed above allows us to exchange $\neg(P \wedge Q)$ with $\neg P \vee \neg Q$ whenever we see that it might be useful. While logical equivalences are in infinite supply, there is a small collection that are so useful that they constitute part of the standard toolkit in mathematical logic. These are often listed under the banner, "Laws of Propositional Logic." Such a list follows.

2.3 Laws of Propositional Logic

Let P, Q, and R denote arbitrary propositions. Each of the following is easily shown (via truth table) to be a tautology.

2.3.1 Associative Laws

(1) $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$

(2) $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$

2.3.2 Commutative Laws

(3) $P \wedge Q \equiv Q \wedge P$

(4) $P \vee Q \equiv Q \vee P$

2.3.3 Idempotency Laws

(5) $P \wedge P \equiv P$

(6) $P \vee P \equiv P$

2.3.4 Absorption Laws

(7) $P \wedge (P \vee Q) \equiv P$

(8) $P \vee (P \wedge Q) \equiv P$

2.3.5 Distributive Laws

(9) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

(10) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$

2.3.6 Law of Double Negation

(11) $\neg\neg P \equiv P$

2.3.7 Identity Laws

(12) $P \wedge T \equiv P$

(13) $P \vee F \equiv P$

2.3.8 Domination Laws

(14) $P \wedge F \equiv F$

(15) $P \vee T \equiv T$

2.3.9 Law of the Excluded Middle

(16) $P \vee \neg P \equiv T$

These laws are frequently used to simplify expressions. For example, exercise 7 in section 1.5 claims that the form,

$$((P \wedge Q) \vee (P \wedge \neg Q)) \wedge (R \vee \neg R),$$

is logically equivalent to a form consisting of a single variable. This is easily shown:

$$\begin{aligned}((P \wedge Q) \vee (P \wedge \neg Q)) \wedge (R \vee \neg R) &\equiv (P \wedge (Q \vee \neg Q)) \wedge (R \vee \neg R) \\ &\equiv (P \wedge T) \wedge T \\ &\equiv P,\end{aligned}$$

where the first equivalence follows from the distributive law (9), the second from two applications of the law of the excluded middle (16), and the third from the two applications of the identity law (12). In our mathematical investigations, we will be using these more implicitly.

3 Exercises

Exercises for Week two, from Gerstein: in §1.4, 1, 2, 4, 7; in §1.5, 1, 3, 4, 5, 6.